

ORIGINAL

AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

## UNITED STATES DISTRICT COURT

for the  
Central District of CaliforniaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)13840 Judd Street  
Pacoima, California 91331

Case No. 17MJ01093

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California  
(identify the person or describe the property to be searched and give its location):

See Attachment A-5

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. I further find that the affidavit establishes reasonable suspicion for a no-knock and announce entry.

**YOU ARE COMMANDED** to execute this warrant on or before 14 days from the date of its issuance  
(not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

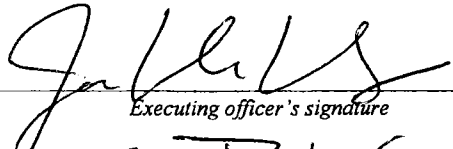
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.  
(name)☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).☐ until, the facts justifying, the later specific date of \_\_\_\_\_Date and time issued: 5/12/17 11:30 a.m.

Judge's signature

City and state: Los Angeles, CaliforniaCHARLES F. EICK, U.S. Magistrate Judge  
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

<b>Return</b>		
Case No.: 17MJ01093 24SG-LA-4937091	Date and time warrant executed: 5/17/17 4:00 AM	Copy of warrant and inventory left with: CARLA MARIA CAAL
Inventory made in the presence of: N/A		
Inventory of the property taken and name of any person(s) seized: [Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]		
PLEASE SEE ATTACHED FBI PD-597 RECEIPT OF PROPERTY TWO PAGES.		
<b>Certification</b> (by officer present during the execution of the warrant)		
I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.		
Date: 5/18/17		
<div style="text-align: right;">             Executing officer's signature            SA JESSE DE LA SIERRA            Printed name and title         </div>		

ATTACHMENT A-5

PREMISES TO BE SEARCHED

The premises to be searched is the parcel located on 13840 Judd Street, Pacoima, California 91331 ("SUBJECT PREMISES 5"). SUBJECT PREMISES 5 is a single family residence located on the southwest corner of Laurel Canyon Boulevard and Judd Street. SUBJECT PREMISES 5 is tan with white trim. The front door is secured by a white security screen door. The numbers "13840" are written in black on a white backdrop and are located to the left of the front door. A driveway is located on the west side of the house, leading to two single car garages with white doors. The house and garage are surrounded by a fence. The side walls of the fence appear to be made of a combination of both chain link and stone. The front of the fence is chain link. There is a pedestrian gate and a vehicle gate within the front portion of the chain link fence.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18 U.S.C. § 1962 (c) and (d) (Racketeer Influenced and Corrupt Organizations ("RICO") Conspiracy and substantive RICO) ("SUBJECT OFFENSES"), specifically:

a. Documents or other items showing occupancy, ownership, or rental of the SUBJECT PREMISES identified on the search warrant, including addressed envelopes, utility bills, telephone bills, rent receipts, keys, or items with labeled or personalized names;

b. Photographs, scrapbooks, images of graffiti associated with MS-13;

c. Posters, drawings, hats or other apparel bearing MS-13 signs and symbols;

d. Rosters, monikers, and telephone numbers for MS-13 members;

e. Notes or papers containing information about discipline as to an MS-13 member, debts owed by MS-13 members, MS-13 members who are not in good standing, rent collection, and rent payments; and

f. Cellular telephones and any forensic copies thereof used to facilitate the SUBJECT OFFENSES used by or in the possession of persons identified by name in Attachments A1-

A30 and pages 3-6 of the affidavit in support of the search warrant.

g. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output

devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

2. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.



d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an

application for such an order is pending). Otherwise, the government must return the device.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

3. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

4. During the execution of this search warrant, the law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of any person, who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, onto the fingerprint sensor of the device (only when the device has such a sensor) in order to gain access to the contents of any such device.

5. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

**UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property**

Case ID: 245Q-LA-4937091On (date) 5/17/17

item (s) listed below were:  
☒ Collected/Seized  
☐ Received From  
☐ Returned To  
☐ Released To

(Name) \_\_\_\_\_

(Street Address) 13840 JUDS STREET(City) PACIFICA, CA 91331

Description of Item (s): \_\_\_\_\_

- 1) T-Mobile Cell Phone (Black)
- 2) Black Samsung Cell Phone
- 3) Papers / Docs
- 4) Mail w/ Address
- 5) Documents
- 6) Documents
- 7) Documents (AUTO)
- 8) Access Documents
- 9) Documents
- 10) Tablet (Black)
- 11) White Cell phone
- 12) Black & Green Cell phone
- 13) Black Flip phone
- 14) Black two lens phone
- 15) Documents
- 16) Black Samsung Flip phone
- 17) Passport & SSN Card
- 18) CA I.D. Card

Received By: MA  
(Signature)Printed Name/Title: SA Marcus McCainReceived From: Carla Coal  
(Signature)Printed Name/Title: Carla Coal

**UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property**

Case ID: 245G-LA-4937091On (date) 5/17/2017

item (s) listed below were:

- ☒ Collected/Seized  
☐ Received From  
☐ Returned To  
☐ Released To

(Name) \_\_\_\_\_

(Street Address) 13840 Tuddel Street(City) Pacoima, CA 91331

Description of Item (s): \_\_\_\_\_

19) SSN Card20) 4 I.D. Cards21) Black AT&T Samsung Cell phone22) Garmin23) Notebook24) Apple I-Phone25) Vehicle Registrations26) 4 Memory Cards27) Black Beaver28) Bible w/ documents29) Documents30) Insurance Doc's31) Insurance Doc's32) Dell Laptop33) White Cell phone (Samsung)34) Black LG Cell phone35) Apple Cell phone Black36) HP Pavilion LaptopReceived By: [Signature]  
(Signature)Printed Name/Title: SA Marcus McCainReceived From: [Signature]  
(Signature)Printed Name/Title: Carla Card